Public Knowledge

May 21, 2019

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114

Dear Ms. Dortch,

On May 17, 2019, Harold Feld, Dylan Gilbert, and Lindsay Stern of Public Knowledge met with Michael Scurato, the Acting Legal Advisor for Media and Consumer Protection to Commissioner Starks, with regard to the above-captioned proceeding.

Public Knowledge expressed the importance of protecting consumer privacy in the proceeding. Public Knowledge spoke about its concerns regarding the recent actions of three major telecom companies -- AT&T, Sprint, and T-Mobile. A Motherboard investigation revealed that these companies sold (or allowed improper access to) highly sensitive customer information that was "intended to be used by 911 operators and first responders to data aggregators."[1] As such, Public Knowledge discussed how it believes that these telecom companies have violated FCC precedent as well as the Communications Act, specifically 47 U.S.C. 222, because under the law "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information" of their consumers. Public Knowledge believes the FCC should investigate these violations.

Public Knowledge discussed the recently submitted letters from AT&T, Sprint, and T-Mobile in response to Commissioner Rosenworcel's letter to each company requesting information regarding its practice of selling location-based information. Each company expressed that its geolocation information is not connected or related to the National Emergency Address Database ("NEAD") and was not improperly used or sold. Specifically, AT&T's letter states: "The FCC's prohibitions on the use of the NEAD for non-emergency services do not apply to A-GPS because A-GPS is not associated with or stored within NEAD." Sprint's letter states: "Sprint's commercial location based services platform does not have connectivity to, nor does it use data from, the NEAD." Additionally, T-Mobile's letter states: "[A]t no time during the existence of T-Mobile's location aggregator program did the Location Aggregators or the downstream location based services providers receive information derived from the NEAD or from 911 calls . . . and while Assisted GPS ("A-GPS") data is important to current 911 functions, there appears to be a misconception in press reports that 911 services are its only source or use."

[1] Motherboard, *Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls*, Feb. 6, 2019, available at https://www.vice.com/en_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls.

Public Knowledge expressed its concern with these sentiments, but was pleased to see that Verizon's letter states that third party entities "no longer have access to Verizon subscriber location information through the aggregators."

The three aforementioned telecom providers expressed that the geolocation information that their companies sold were not NEAD information and thus not subject to heighted privacy protections. However, whether the sold information was or was not NEAD information is missing the point and is not particularly relevant when it comes to carriers protecting their consumers' information. Even if it is true that the information was not NEAD information, FCC precedent shows that this type of information is still customer proprietary network information ("CPNI") and is subject to the heighted privacy protections under 47 U.S.C. 222, including the obligation to protect the confidentiality of CPNI.

In the FCC's *Fourth Report and Order* ("2015 Order"),[2] the Commission articulated the following:

> "In addition to the NEAD Privacy and Security Plan, we believe that certain explicit requirements on individual CMRS providers are necessary to ensure the privacy and security of NEAD data and any other information involved in the determination and delivery of dispatchable location. We require that, as a condition of using the NEAD or any information contained therein to meet our 911 location requirements, and prior to use of the NEAD, CMRS providers must certify that they will not use the NEAD or associated data for any purpose other than for the purpose of responding to 911 calls, except as required by law. ***Additionally, should aspects of a CMRS provider's dispatchable location operations not be covered by the NEAD privacy and security plan, the provider should file an addendum to ensure that the protections outlined in the NEAD plan will cover the provider's dispatchable location transactions end-to-end.***" (emphasis added).[3]

Moreover, the 2015 Order stated: "In light of the Section 222 exception for 911 calls and the required certification by CMRS that NEAD data will only be used for 911 location purposes, nothing in this Fourth Report and Order should be construed to permit any use of customer or location information stored in the NEAD in any other context."[4]

As seen by the 2015 Order, the FCC has explained that enhanced 911 geolocation data is indeed related to NEAD. This information can only be released pursuant to 911 exceptions, and otherwise it is CPNI information that must not be released as it is protected under heightened security. According to the 2015 Order, carriers must put in place necessary security procedures so that this confidential customer information is not disclosed unless otherwise required by law.

As a result of legal precedent found in both the Communications Act and FCC rulemaking, Public Knowledge explained that even if carriers sold geolocation information that is not

---

[2] In the Matter of Wireless E911 Location Accuracy Requirements, *Fourth Report and Order*, PS Docket No. 07-114, released Feb. 3, 2015 ("2015 Order").
[3] *Id.* at ¶ 71.
[4] *Id.*

technically NEAD information, CPNI requires that carriers take reasonable measures to protect this sensitive information.

Public Knowledge highlighted critical FCC precedent. In 2007, under Chairman Kevin Martin, the Commission released its *Report and Order* ("2007 Order") regarding telecommunications carriers' use of CPNI.[5] In the 2007 Order, the Commission explained that under Section 222 of the Communications Act, "Congress accorded CPNI . . . the greatest level of protection under this framework."[6] The 2007 Order explained that CPNI includes information such as the phone numbers called by a consumer, the frequency, duration, and timing of these calls, and any services purchased by the customer. As such, CPNI "includes some highly-sensitive personal information," and under Section 222(c)(1), a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances: (1) as required by law; (2) with customer's approval; or (3) in its provision of the telecommunications service from which such information is derived.[7] In addition, the 2007 Order explained that under the Commission's rules, telecommunications carriers must receive consent before disclosing CPNI to joint venture partners and independent contractors for the purposes of marketing services to customers, and that the Commission's safeguard rules requires carriers to maintain records that track access to customer CPNI records and maintain a record of all instances where CPNI was disclosed or provided to third parties.[8]

Moreover, Public Knowledge explained how the 2007 Order requires telecommunication carriers subject to CPNI rules to maintain appropriate technology protections. As the 2007 Order states: "We also codify the existing statutory requirement contained in Section 222 of the Act that carriers take reasonable measures to discover and protect against activity that is indicative of pretexting" and that the "adoption of the rules in this Order does not relieve carriers of their fundamental duty to remain vigilant in their protection of CPNI, nor does it necessarily insulate them from enforcement action for unauthorized disclosure of CPNI."[9] The Commission reminded carriers that the Communications Act imposes on them "the duty of instituting effective measures to protect the privacy of CPNI," and emphasized that carriers are required to "take *reasonable steps* to protect their CPNI databases from authorized attempts by third parties to access CPNI." (emphasis added).[10]

The sale of CPNI as revealed in the Motherboard news story evidences the reality that reasonable privacy protections are likely not in place in many telecom companies. To reiterate, whether the A-GPS information is or is not in the NEAD database is not an important distinction. Either way, carriers should not have disclosed or sold this information to third parties.

---

[5] In the Matter of Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, *Report and Order and Further Notice of Proposed Rulemaking*, CC Docket No. 96-115, released Apr. 2, 2007 ("2007 Order").
[6] *Id.* at ¶ 4.
[7] *Id.* at ¶¶ 5-6.
[8] *Id.* at ¶¶ 8-9.
[9] *Id.* at ¶ 33.
[10] *Id*. at ¶¶ 35-36.

The arguments of the carriers lead to the absurd result that no customer information is truly protected because if anyone gives sensitive information to the carriers, in theory the carriers can make a copy of the information, use it for their own purposes, and *then* put it into the NEAD database. If this were the case, third parties could not turn over information needed to populate the NEAD because that information would not be secure. This is not the type of system we want to live in nor is it one that Congress or the Commission intended.

In sum, the government and the Commission did not intend to create a "no man's land" for certain information to sit in limbo between that of CPNI and NEAD. Public Knowledge supports the goal of enhancing 911 geolocation data, but the Commission must make sure that as the geolocation of a consumer becomes more precise, consumer privacy is still strongly protected. Enhancing 911 geolocations should not be a government mandate that lets carriers harvest and sell their customers information in a way that violates legal and regulatory precedent. As a result, the Commission must investigate carriers to see if they broke the law by not having sufficient privacy protections as required under the law, and it also must clarify the need for privacy protections in the "z-axis proceeding." The Commission must clarify that whether information is classified as NEAD or not, geolocation data is still CPNI and therefore carriers cannot use or sell it unless otherwise required by law.

Respectfully submitted,
/s Lindsay Stern

Lindsay Stern
Policy Fellow
Public Knowledge
1818 N Street NW, Suite 410
Washington, D.C. 20036
(202) 861-0020

Cc: Michael Scurato